DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC Supplement 1 to AR 190-13

1 December, 2000

Military Police

THE ARMY PHYSICAL SECURITY PROGRAM

Applicability. This supplement applies to Headquarters (HQ), U.S. Army Materiel Command (AMC); major subordinate commands (MSC); their subordinate installations and activities, to include Government-owned contractor-operated (GOCO) facilities; Contractor-owned, contractor- operated facilities (only when specifically addressed in this supplement); and separate installations and activities reporting directly to HQ AMC.

Supplementation. Approval for this supplement was granted 20 September 2000 by Headquarters, Department of the Army (HQDA) (DAMO-ODL). Further supplementation of this regulation is prohibited unless prior approval is obtained from HQ AMC (AMCPE-S). When supplements are approved and issued, one copy of each will be furnished to HQ AMC (AMCPE-S), and Chief, AMC Security Support Division (SSD), ATTN: AMXMI-SD.

AR 190-13, 30 September 1993, is supplemented as follows:

Page i, Proponent and exception authority. Add the following at the end:

Deviation from mandatory standards and procedures is permitted only when a waiver or exception has been granted. Requests for waiver or exception to this regulation will be submitted to the Deputy Chief of Staff for Operations and Plans, ATTN: DAMO-ODL-S, 400 Army Pentagon, Washington, DC 20310-0400, through the Commander, U.S. Army Materiel Command, ATTN: AMCPE-S, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001. All requests for waiver or exception must contain sufficient justification, compensatory measures with cost estimates, and be submitted in the format prescribed in appendix G of this supplement. Outside continental United States (OCONUS) AMC elements, supported by host-tenant agreements, will forward waiver/exception requests through their host-tenant headquarters and provide an information copy of the request to their respective major subordinate command (MSC), and this headquarters.

Page ii, Appendixes. Add the following:

F. Physical Security Plan/Plant protection Plan
G. Physical Security Waivers and Exceptions
H. Responses to Physical Security Survey (PSS)/Information Security Program Inspection (ISPI) Reports

Page 4, paragraph 1-23. New paragraph title should read:

"Commanders of Major Subordinate Command (MSC) Headquarters, installations or activities"

---

*This supplement supersedes AMC Supplement 1, 22 September 1995, to AR 190-13, 30 September 1993

Page 4, paragraph 1-23b. Add at the beginning of first sentence:
"MSC Headquarters commanders and …"

Page 4, paragraph 1-23b(3). Add the following at the end:

Installation physical security plans or plant protection plans will be signed by the installation commander or contracting officer's representative (COR), as appropriate. Field operating activity plans, if required, will be signed by the head of the activity. Plans applicable to GOCO facilities will identify all security directives necessary to function under the operating contract plant protection clause. AR 190-13, appendix A, will be used as a guide in identifying appropriate security directives. MSC Provost Marshal/Security Officer will review the plant protection clause to ensure applicable directives are contained therein prior to approval of GOCO facility contracts by the contracting officer.

Page 4, paragraph 1-24b. Add subparagraphs (7) through (10):

(7) Commanders or civilian directors of MSCs, installations, and separate reporting activities are responsible for implementation of policies and procedures established by this regulation. AMC tenant activities will comply with host installation policies and procedures per negotiated support agreements. However, internal functions will be governed by pertinent policies and procedures specified in this regulation. Commanders will appoint a security officer to supervise and administer the security program for their organizations.

(8) Commanders or directors located on non-AMC installations or in GSA-leased or owned facilities will ensure necessary security considerations are included in applicable memoranda of understanding, contracts, or support agreements.

(9) Commanders of AMC installations with tenant activities will ensure support agreements with the tenants clearly delineate the security requirements of both parties.

(10) Copies of those portions of support agreements which define security responsibilities will be retained by the respective Security Officer.

Page 5. Add paragraph 1-28:

The Chief, AMC SSD, will conduct Physical Security Surveys (PSS) of AMC installations and activities.

Page 5, paragraph 2-1. Add subparagraph d:

d. Similarly, product physical security requirements must be fully integrated into the acquisition process to protect materiel located at contractor facilities for which AMC is responsible. This will be accomplished by ensuring applicable Department of the Army, e.g., AR 190-11, AR 190-13, etc., and Department of Defense (DOD) manuals, instructions, and regulations e.g., DOD 5100-76-M, etc., are incorporated into all production or supply contracts to be performed at contractor-owned, contractor-operated (COCO) facilities.

Page 5, paragraph 2-1b. Add the following at the end:

Within AMC, responsibility for conventional physical security programs rests with installation commanders. Within the European Theater, responsibility for physical security programs rests with U.S. Army, Europe (USAREUR) Area Support Group (ASG) commanders per an existing memorandum of understanding (MOU) between HQ AMC and USAREUR. Overall operational responsibility for the physical security program will be a critical element in provost marshal and security officer performance standards.

Page 5, paragraph 2-4d. Add the following at the end:

Arms, ammunition, and explosive storage facilities or areas and demilitarization facilities or areas (excluding open burning grounds and demolition ranges) will be designated as mission-essential or vulnerable (MEVA) areas. Commanders may add other facilities deemed appropriate, as long as they meet the requirements outlined in paragraph 2-4 of AR 190-13. Guidance in AR 380-19 and AMC Supplement 1 thereto will be followed in the designation of data processing locations and facilities.

Page 6, paragraph 2-8. Add subparagraph c:

c. Commanders, Chiefs, or Directors of AMC activities located on any DOD installation will determine if an installation-wide threat statement has been developed that includes their activities. If not, a local AMC threat statement will be prepared. Local threat statements may also be prepared if host statements are considered to be inadequate. AMC host installations will include tenants in installation-wide threat statements. Tenants will be included in the review of statements to ensure their security concerns are addressed. Statements will be updated whenever significant changes to the threat posture occur.

Page 6, paragraph 2-9. Add the following at the end:

Installations will use the expanded format depicted in appendix F of this supplement. All tenant activities on AMC installations will be included in the host physical security plan. Those AMC tenant activities located on non-AMC installations will forward their MEVA list and list of restricted areas to the host installation for inclusion in the host physical security plan. Plans/plant protection plans will be kept current, and a copy, to include changes or revisions, will be furnished to SSD (AMXMI-SD), which serves as office of record for all AMC plans. Instances where security standards imposed by AMC or one of its intervening commands are greater than those required by a non-AMC host, the AMC physical security requirement will apply.

Page 7, paragraph 2-10(c). Add the following at the end:

Within AMC, physical security surveys will be scheduled by Chief, SSD every 24 months for activities storing conventional AA&E.

Page 7, paragraph 2-10d. Add the following at the end:

Reports of corrective actions resulting from PSSs will be forwarded through command channels to SSD (AMXMI-SD). AMC elements located in the European Theater will forward reports of corrective actions resulting from PSSs through AMC-Europe (AMXEU- OPI) and the Commander, Operations Support Command

Command (AMSOS-SC) to SSD (AMXMI-SD). Information copies will be provided to USAREUR (AEAPM-O-PS). Installations or activities will respond to survey reports within 90 calendar days from date of formal report. Suspense dates for subsequent responses will be established by SSD, as appropriate. Responses will be per appendix H of this supplement.

Page 8, paragraph 2-12. Add the following at the end:

SSD conducts PSS's of all AMC installation/activities. Therefore, SSD (AMSMI-SD) will review the surveyed installation's or activity's security inspection reports, as well as the overall effectiveness of the physical security inspection program. An evaluation of these programs will be included as a part of the PSS of the installation or activity. These records will be maintained in active files until completion of the next physical security survey. Within the European Theater, the ASG and/or Base Support Battalion (BSB) is responsible for conducting physical security inspections of all tenant activities. Copies of security inspection reports received by AMC elements will be forwarded to AMC-Europe (AMXEU-OPI).

Page 13, paragraph 3-2b. Add the following at the end:

Civilians will receive the same or comparable resident training courses specified for military inspectors. These civilians will be cleared for access to SECRET national defense information before being issued physical security inspector credentials and before conducting physical security inspections.

Page 14, paragraph 3-4b. Add subparagraph (6):

(6) Physical security inspector credentials will be issued to selected AMC physical security inspectors by the AMC Command Provost Marshal (AMCPE-S).

Page 17, paragraph 4-7d(2). Add the following at the end:

Requests for purchase, issue, lease, or lease renewal of nonstandard physical security equipment (PSE) will be processed as indicated in paragraphs 4-7d(3) and 4-7(d)5 of this supplement.

Page 17, paragraph 4-7d(3). Add the following at the end:

PSE projects to be funded with management decision package (MDEP) monies, (e.g., VTER, QLPR, RJC6, etc.) will be formalized into functional criteria packages and forwarded through the appropriate MSC to Commander, Installation and Services Activity (I&SA), ATTN: AMXEN-C, Rock Island Arsenal, IL 61299-7190, for PSE review and approval. Concurrent submissions will be made to the SSD, ATTN: AMXMI-SD, to assist in the PSE review process. Submissions also will be made to appropriate elements of the U.S. Army Information Systems Command. I&SA will consolidate all review comments and forward the approved criteria package to the appropriate district engineer. I&SA is responsible for coordinating with appropriate AMC elements to ensure those required to participate in pre-design conferences are invited on a timely basis. Projects specifying issue, purchase, lease, or lease renewal of nonstandard PSE must be supported by information required in paragraph 4-7d(5)(d) of this supplement.

Page 17, paragraph 4-7d(3)(b). Add the following at the end:

A security engineering survey (SES) (para 2-14, AR 190-13) will be performed when planning any new construction or renovation or upgrades to existing facilities where there are likely to be physical security requirements. The scope of the security engineering survey will be determined by the magnitude of the project. A copy of the SES results when conducted in support of PSE projects described in paragraphs 4-7d(1), (2), and (3) of the regulation and this supplement, will be provided to the SSD, ATTN: AMXMI-SD, to facilitate the PSE review process.

Page 17, paragraph 4-7d(3)(c). Add the following at the end:

Requests for SESs beyond the capability of the installation will be forwarded through the MSCs to the AMC SSD, ATTN: AMXMI-SD, with copies furnished to I&SA, ATTN: AMXEN-C. SSD will review the request for completeness, will conduct those within its capability, and will forward others to I&SA, who is responsible for coordinating with HQ, U.S. Army Corps of Engineers. Requests for SESs for AMC elements located in the European Theater will be forwarded to AMC-Europe, ATTN: AMXEU-OPI. AMC-Europe will coordinate the request with USAREUR Provost Marshal to ensure inclusion of the project into USAREUR's funding forecast for intrusion detection systems (IDS). Within AMC, funding for SESs is the responsibility of the requesting installation.

Page 17, paragraph 4-7d(3)(d). Add the following at the end:

Within AMC, funding for site surveys is the responsibility of the requesting installation.

Page 17, paragraph 4-7d(5)d. Add the following at the end:

To facilitate the technical review and approval by HQ AMC, justifications for issue, purchase, lease, or lease renewal of nonstandard PSE will be forwarded through the appropriate MSCs to SSD, ATTN: AMXMI-SD.

Page 19, paragraph 4-13. Add subparagraph d and e:

d. Develop instructional materials and train security personnel to operate the system. Further, provide training to employees working in protected areas so they will be familiar with the system in use.

e. Prepare an IDS standing operating procedure (SOP) which includes procedures for responding to alarms. DA Form 4930-R (Alarm/Intrusion Detection Record), contained in the Glossary, Physical Security Update 10-3, will be used to record all alarms. A computer-generated printout of alarms may be used as a substitute provided all required information on the DA Form 4930-R has been included or supplemental information is included in a log. The SOP also must address operation of the monitor console, control of operational and maintenance keys, and procedures for testing and maintaining the system. Unless more stringent requirements are imposed by Army regulations, security or operational personnel will conduct quarterly operational checks of all sensors. Where advanced sensor systems provide the capability to remotely stimulate individual sensors, via an electronically activated sensor phenomenology device, this capability may be used to fulfill testing requirements. Annual maintenance inspections will be made by organizations or personnel designated to service the system. This will be a complete system evaluation to ensure it meets manufacturer’s performance

standards. Documentation of the above tests and inspections will be kept on file until the next test or inspection is accomplished.

Page 20, paragraph 5-1. Add subparagraph c:

c. Where security identification cards or badges are used as a method of personnel movement control for a designated and posted restricted (i.e., controlled, limited, or exclusion) area, they will be issued to all personnel entering that area.

Page 20, paragraph 5-2. Add subparagraphs g through p:

g. Security identification cards or badges issued to assigned military, civilian, and contractor employees will be photographic. Further, contractor employees will be issued distinctive color-coded badges, which clearly differentiate them from government personnel. Badge inserts produced by means of an instantaneous photographic process may be used. Inserts manufactured by this means will employ different and easily distinguishable. This may be accomplished by means of colored backdrops for the holder's photograph, colored inserts, colored tapes, or similar devices that indicate the category of holder, e.g., employee, visitor, vendor, or contractor. Unless otherwise directed by a non-AMC host installation, contractor badges will be pink in color. Cards and badges will be laminated or sealed to preclude tampering or alteration and will have attachments that permit fastening to clothing or suspension around the bearer's neck. The card or badge will be worn above the waist on the front of the body and will be worn at all times while the bearer is within an area requiring identification, unless safety or security considerations dictate otherwise. Security identification cards and badges will not be worn or otherwise used for identification purposes outside the areas for which they were issued.

h. New photographs will be made when there is significant physical change in facial appearance.

i. Nonphotographic temporary employee badges will be issued to permanent employees who have forgotten or lost their photographic employee badge. Temporary badges will be valid for 24 hours or less.

j. Nonphotographic visitor badges will reflect "Escort Required" or "No Escort Required" stamped or printed across the face of the badge. This indication of escort requirement will be of a distinctive size and color to allow easy discernment. All visitor badges will be distinctly marked with a large "V." At a minimum, the "V" must be of the size recommended for photographs on badges issued to assigned personnel, i.e., 1 inch wide and 1-5/16 inches in height.

k. Registers reflecting the issue of nonphotographic visitor badges will be maintained. These registers will reflect the recipient’s name (printed and signature), organization, phone number, area to be visited, date and time in, date and time out, badge number, and name of escort, if applicable. Registers will be destroyed 6 months after conclusion of visit and return of badges.

l. Issued security badges will not be duplicated, used for identification outside the areas for which they were issued, or have items affixed which obscure any portion of the badge.

m. Badges maintained at entrance and exit points will be inventoried jointly each time responsibility for the custody of badges is changed and at the beginning and end of each duty day or shift. All badges not accounted for will be reported immediately to the provost marshal or security officer. A written record of inventories will be maintained and destroyed after 6 months, unless discrepancies are reflected or more stringent procedures are required by other Army regulations. Inventory records showing evidence of lost or unaccounted for badges will become a part of the investigative files concerning the incident. When badges are left unattended, they will be locked in containers of at least 20-gauge steel or material of equivalent strength. Containers will be secured to the structure to preclude easy removal and in locked buildings or rooms with structural features that minimize the likelihood of unauthorized entry. Containers will be secured with a lock meeting or exceeding Commercial Item Description (CID) A-A-1927 -- Grade II, Class 1, Type A or an approved 3-position combination padlock, i.e., GSA approved changeable combination padlock built to Federal Specifications FF-F-110 (Sargent and Greenleaf Model 8077AD).

n. Badge inserts will be serially numbered when printed or immediately upon receipt and will include the following statements:

(1) "Property of the United States Government."

(2) "Postmaster: Postage guaranteed. Return to (name and address of command)."

(3) "Warning: Issued for official use of holder designated hereon. Use or possession by any other person is unlawful and will make offender liable to heavy penalty. Title 18, U.S. Code, Sections 499 and 701."

(4) "Loss of this badge must be reported at once."

o. When rebadging the entire system, replacement security badges will be of a different design or color to ensure easy differentiation between the old and new issues.

p. The use of security identification cards and badges, other than the two types (photographic and nonphotographic) described above, is prohibited.

Page 20 paragraph 5-3. Add subparagraph 5-3.e.

e. Procedures for control and accountability of cards and badges will, as a minimum, include --

(1) Appointment by the installation or activity commander in writing, of a security credential custodian (and assistants), and written procedures for issue, turn-in, recovery, and destruction.

(2) Annual 100 percent unannounced inventories will be conducted by a disinterested person(s) appointed in writing. A written record of the inventory and inspection will be provided to the Provost Marshal/Security Officer (PM/SO) and will be kept on file for 1 year. Unannounced inspections, which will review compliance with local badging procedures contained in AR 190-13, and this supplement, paragraphs 5-1 through 5-4, may be conducted by personnel within the PM/SO, as long as the person is not within the direct rating chain of the person being inspected. Written

appointment is not required; however, a written report will be provided to the PM/SO and will be retained on file for 1 year. Unannounced inspections will not be conducted within 30 days preceding or following the semiannual inventory.

(3) Maintenance of a current and complete register of all security credentials reflecting numbers on-hand, numbers issued, and to whom, and other disposition, e.g., lost, mutilated, or destroyed.

(4) Prompt invalidation of lost credentials. A current listing of these documents will be provided to all on-shift security personnel for their use in verifying access to areas in which security badges are required to be worn.

(5) Prompt recall and destruction (within 60 days) of mutilated, defective, or obsolete badges.

Page 20, paragraph 5-4a. Add the following at the end:

Restricted controlled area badges must be replaced no later than 5 years from the date of issue or when 10 percent are unaccounted for or lost.

Page 21. Add paragraph 5-5, 5-5a, and 5-5b:

5-5. When entry control rosters (ECR) are used for controlling entry into restricted areas, ECR will be --

a. Kept current and revalidated at least every 12 months by the installation provost marshal, security officer, or designated representative.

b. Changes to ECR will be in writing and signed by the Security Officer or designated representative. Changes will be issued by the appropriate authority immediately upon notification of additions or deletions. Pen and ink changes are authorized. Signatures of individuals making pen and ink changes will be annotated on rosters. Signature cards will be maintained at access points for persons authorized to sign ECRs and changes thereto.

Page 22. Add paragraph 6-7.

6-7. Restricted Area Physical Security Standards for Restricted Areas not already addressed by other regulations.

a. Minimum physical security standards for restricted (exclusion) areas are --

(1) Access limitations. All visitors, including maintenance and support personnel who are required to enter the area to perform essential repairs or similar functions, will be escorted at all times to preclude their access to classified or other sensitive material.

(2) Access authority. Access lists or entry control rosters are mandatory. Positive identification is required in conjunction with the access list or entry control roster. The number of persons authorized access will be kept to a minimum.

(3) Access controls. Security personnel will be posted at entry

points during operational hours. Security personnel will be posted or protective alarms will be activated at entry points during nonoperational hours. A badge exchange system will be used under the direct control of security personnel at entry points. Operating personnel may control access at classified communications facilities and within exclusion areas under the provisions of ARs 190-54, and 190-59. The necessity for badge exchange procedures will be determined locally for such facilities.

(4) Protective barriers. Protective barriers are mandatory for the entire perimeter. At a minimum, FE-6 chain-link fencing will be used and walls, floors, ceilings, and roofs forming parts of barriers must provide protection equal to FE-6 chain-link fencing. Opaque barriers will be used, as necessary, to preclude visual compromise of sensitive or classified material.

(5) Protective lighting. Protective lighting with an auxiliary power source is mandatory. Perimeter barrier clear zones will be illuminated.

(6) Intrusion detection system (IDS). IDS is required on building entrances and in areas or rooms where protected material is stored.

(7) Posting of signs. Signs meeting the criteria established in basic regulation, paragraph 6-4c, will be posted per paragraph 6-4a.

(8) Security patrol requirements.

(a) Where facilities are protected by IDS, checks by security personnel at intervals not exceeding 4 hours are mandatory.

b. Minimum physical security standards for restricted (limited) areas are --

(1) Access limitations.

(a) For areas containing classified material, only personnel with an official need-to-know and appropriate security clearance will be allowed unescorted entry. All other persons will be continuously escorted.

(b) For areas containing high-dollar-value or sensitive material, an official purpose and positive identification must be determined. Escort requirements will be established locally.

(2) Access authority. Access lists, entry control rosters, or an authorized badge system may be used as determined by the Security Officer.

(3) Access controls. Security personnel, receptionists, supervisory operational personnel, or electromechanical access devices will control entry points.

(4) Protective barriers. Barriers are recommended for the entire perimeter. Fencing, if used, will be, at a minimum, FE-1 (CE Drawing 40-16-02). Buildings may be part of the barrier so long as the structural features provide protection equal to FE-1 barbed wire fencing. Opaque barriers will be used, as necessary, to preclude visual compromise of classified or sensitive material.

(5) Posting of signs. Posting of signs will be per AR 190-13, paragraph 6-4.

(6) Security patrol requirements.

(a) Where the area is not protected by IDS, security personnel inspection is mandatory every 4 hours during nonoperational periods.

(b) Where the perimeter barrier or all interior facilities requiring protection have IDS, security personnel inspection is mandatory every 8 hours during nonoperational hours.

(c) Where the perimeter barrier and interior facilities have IDS, security patrol frequencies will be determined locally.

(d) Each structure or room containing a security interest will be physically checked at least once during each shift when not occupied by operational personnel.

c. Minimum physical security standards for restricted (controlled) areas are --

(1) Access limitations. Personnel with an established need to enter.

(2) Access authority. As determined by the commander.

(3) Access controls. Security personnel, receptionists, operational personnel, or electromechanical access devices may be used to control entry points when determined necessary by the commander. An authorized badge system will be utilized.

(4) Protective barriers. Fencing should be considered for movement control purposes, but will be installed only when deemed appropriate by local commanders to protect property or material for which they are responsible.

(5) Posting of signs. Posting of signs will be per AR 190-13, paragraph 6-4.

(6) Security patrol requirements. Required at intervals not to exceed 8 hours during nonoperational periods. Patrol frequency during operational hours will be determined locally.

Page 23. Add Chapter 9:

Chapter 9

ADDITIONAL SECURITY REQUIREMENTS

9-1. Use of Seals.

a. Strict seal accountability is mandatory. Accountability starts with the manufacturer and ends with seal destruction. Seals, to be effective, must meet two basic requirements as to construction and accountability:

b. Seal construction.

(1) Seal will be strong enough to prevent accidental breakage during normal use.

(2) Seal design will be sufficiently complex to make unauthorized manufacture of a replacement seal difficult.

(3) Seal will provide readily visible evidence of tampering and preclude reconstruction after the seal is broken.

(4) Individual serial numbers will be embossed on each seal.

c. Seal accountability.

(1) Each seal will be strictly accounted for from manufacture to the time of application.

(2) Seal custodians, persons authorized to apply seals, and persons authorized to remove seals, will be appointed in writing by the installation or activity commander, or persons designated to exercise that authority by the commander. These appointments will be kept to a minimum.

(3) Seals will be ordered or purchased from manufacturers by a single office within each organization and will be recorded serially in a log by the seal custodian. As an alternative, seals may be ordered by a single office on an installation and provided to subordinate and tenant elements on the installation per a documented agreement. Such an agreement must clearly delineate the responsibilities of both parties.

(4) Until issued to users, all seals will be safeguarded in a suitable locked metal container, limiting access, and under supervision of the custodian in a manner that will prevent unauthorized substitution or illegal use of seals.

(5) Seals not issued for actual use will be inventoried monthly by serial number and a record of same maintained.

d. Issuing seals to users.

(1) Custodians will issue seals to users, obtain a receipt, and record issuance by serial number.

(2) Each seal user will maintain a hard cover log book showing numbers of all seals and the date received.

(3) Each user will sign for the seals by number and after application prepare a seal application log showing seal number, date and time applied, identification of item to which applied, and the name of the authorized person applying the seal.

e. Seal application and verification.

(1) Seal numbers will be entered in the designated place on pertinent transportation documents, e.g., bills of lading, gate passes, manifests, and in the user's seal application log.

(2) Trailers will be sealed as soon as the load is complete.

(3) Gate guards will check seal numbers against gate passes and shipping documents and note seal numbers, along with vehicle identification data, on the gate log.

(4) Persons receiving sealed shipments or equipment will examine the seal and record the number on the receipt.

(5) Whenever a seal is removed, broken, or suspected of having been compromised, the following actions must be accomplished.

(a) Record pertinent information including date and time seal was removed, broken, or discovered broken; by whom; organization name; circumstances and justification for breaking the seal; new seal number, if applied; and person resealing.

(b) Make proper disposition of broken seals, which will be retained until it is determined whether the shipment contains discrepancies. If there are none, the seal will be destroyed. If any discrepancy is found, the broken seal will be sent to the Security Officer. If the shipment contains classified information, material, or equipment, the following actions will be immediately initiated: Secure the area, notify the commander of the activity, contact the local military intelligence support office. Authorized personnel will conduct an immediate inventory of the classified material.

9-3. Control of movement and access by visiting contractor representatives.

a. It is vital to the proper conduct of procurement actions that contractor representatives not have intentional or inadvertent exposure to bidding or project information that provides an unfair advantage to a particular firm in its efforts to acquire Government contracts.

b. At a minimum, areas in which contractual processes are accomplished will be designated and posted as restricted (controlled) areas. This designation and posting of the areas requires that practical, positive procedures be implemented to identify and control personnel entering, departing, and moving within such areas. Particular attention must be given to procedures concerning visitor registers, badges, and escort requirements for persons who are provided access to these restricted areas.

c. While officials of various firms may have need for recurring access to areas in which procurement functions are accomplished, convenience alone must not be the basis for unescorted entry into such areas. Unescorted access will be permitted only when sponsoring activities can show a demonstrable recurring access requirement for a specified period of time, and for a purpose which will clearly further the conduct of U.S. Government business.

Page 29. Add appendixes F, G, and H.

The proponent of this memorandum is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQAMC, ATTN: AMCPE-S, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL:

CHARLES C. CANNON, JR.
Major General, USA
Chief of Staff

Carolyn Gebre
Acting Chief, Printing and
Publications Branch

DISTRIBUTION:
Initial Distr H (43) 1 ea HQ Acty/Staff Ofc
B LEAD (SDSLE-DOI) (2)
AMCIO-I-SP stockroom (50)

APPENDIX F

PHYSICAL SECURITY PLAN/PLANT PROTECTION PLAN

Copy No.
Issuing Headquarters
Place of Issue

1. Purpose. Briefly state object of plan.

2. Security areas. Refer to and attach as annexes documents designating and defining security areas and mission essential or vulnerable areas (MEVAS). MEVAS must be prioritized in order of criticality.

3. Control measures. Describe access movement controls for personnel, vehicles, and materiel into, within, and out of security areas.

a. Personnel access. Describe controls pertinent to security areas, to include --

(1) Access limitations (who can enter).

(2) Access authority (who can authorize access).

(3) Access controls (describe control, enforcement, badges, and lists).

b. Vehicle controls (to include rail). Describe --

(1) Controls for entrance and exit of vehicles.

(2) Parking controls.

(3) Policy on search of vehicles.

c. Materiel control. Describe incoming and outgoing procedures for --

(1) Documentation examination.

(2) Controlling admission and exit.

(3) Search and inspection.

(4) Special controls on delivery or release of supplies.

(5) Classified shipments.

4. Physical barriers. Describe or list --

a. Installation perimeter and security area barriers.

b. Gates (hours of operation and security requirements).

c. Clear zones (criteria and maintenance).

d. Signs (type and posting).

e. Inspection and maintenance responsibility.

5. Protective lighting. Describe or list --

a. Security areas where used.

b. Purpose and systems in use.

c. Actions to be taken in the event of power failures.

d. Auxiliary lighting (to include secondary or emergency power sources).

e. Inspection and maintenance responsibilities.

6. Intrusion detection systems. Describe or list --

a. Security areas where used.

b. Purpose and type of system in use.

c. Monitoring procedures (to include use of logs and registers).

d. Responses to be made in the event of an alarm.

e. Testing and inspection requirements.

f. Actions to be taken in the event of power failures.

g. Auxiliary (secondary or emergency) power sources.

h. Maintenance responsibilities.

7. Protective communications. Describe or list --

a. Types and locations.

b. Use.

c. Authentication requirements.

d. Maintenance and testing responsibilities.

e. Auxiliary (secondary or emergency) power sources.

8. Lock and key control. Describe or list --

a. Administrative and supervisory control procedures.

b. Systems and subsystems (number and location).

c. Types of locks used by systems.

9. Security forces. Describe or list --

a. Composition and organization (attach organizational chart as annex).

b. Areas of responsibility.

c. Tours of duty.

d. Uniforms, equipment, and arms.

e. Location of guard posts and patrols to include supervisors (attach as annex).

f. Special orders (attach as annex).

10. Emergency Actions. Indicate emergency actions of general application. Attach, as annexes, detailed plans such as disaster, bomb threat, and antiterrorism.

11. Coordinating instructions. Indicate matters that require actions by other military or civil agencies, to include --

a. Mutual assistance plans with host, tenant, nearby military installations, or civil authorities.

b. Liaison activities with local, state, and Federal agencies and military organizations.

SIGNATURE (Commander)

*Appendixes

A. Installation threat statement.

B. Natural disaster plan.

C. Bomb threats plan.

D. Installation closure plan.

E. Work stoppage plans.

F. Information Systems security plan.

G. Antiterrorism Plan.

H. Resource plans to meet minimum essential physical security needs.

I. Civil disturbance plan.

J. Communication plans.

K. Listing of all DOD/DA/AMC security directives necessary to function under the operating contract plant protection clause. (Note: This appendix is applicable only to GOCO facilities.)

*Annexes too bulky to be included with the plan, as well as those that are classified, will be identified by an insert showing their location.

APPENDIX G

PHYSICAL SECURITY WAIVERS AND EXCEPTIONS

G-1. Waivers provide only temporary relief from compliance with prescribed standards. Requests for waivers are appropriate if corrective actions can be accomplished reasonably by local administrative or work order action or by the initiation of a construction project.

G-2. Waivers: Waivers will be approved for a period not to exceed three years or the time needed to correct the condition(s), whichever is soonest. Whenever conditions or compensatory measures change, an amendment to change the waiver must be submitted, to the approving authority (DAMO-ODL), within 30 days of the change. When conditions remain unchanged for the duration of the waiver, a request for extension is required. Waivers may be extended for up to three years under the same provisions listed above.

G-3. Exceptions generally provide permanent relief from regulatory requirements. Requests for exceptions will be approved only when correction of a deficiency is not feasible and when security afforded by alternative measures or procedures are equivalent or better than that provided by the standard criteria.

G-4. Exceptions: Exceptions will be granted on a permanent basis when it is known deficient conditions cannot be corrected due to resource requirements, physical limitations, etc. However, qualified physical security inspector personnel, on a regular basis, will make a concerted effort to ensure original compensatory measures are in place and are being complied with. Whenever conditions or compensatory measures change, a request for amendment must be submitted to the approving authority (DAMO-ODL) within 30 days for change. Requests for extensions of approved exceptions to Army physical security regulations will not be forwarded to HQ AMC. AMC Security Support Division (SSD) will review the exception during the course of a PSS. SSD will verify that existing condition(s) still require the exception, and that approved compensatory measures are in effect. The results of the SSD review will be recorded in the official evaluation report, and serve as official revalidation. SSD will subsequently notify HQ AMC by separate correspondence in order to ensure revalidations are entered into the database.

G-5. PSS's and inspections will include a review of all waivers and exceptions to ensure that conditions described in the waiver/exception request were accurate and that compensatory measures have been fully implemented. The PSS or inspection report will include a comment regarding the results of that review.

G-6. Requests for issuance of physical security waivers or exceptions will be signed by the commander of the installation, field operating activity, or separate reporting activity originating the request. Separate reporting activity is defined as an AMC element which is not an installation or activity subordinate to an intervening headquarters, but one which reports directly to HQ AMC. If the commander is a general officer, the request may be signed by the deputy commander or chief of staff.

G-7. Except for separate reporting activities, all requests will be submitted to intervening commands for review and endorsement prior to submission to HQ, AMC. All endorsements will recommend approval and provide the rationale for the recommendation. Endorsements will be signed by the

commander of intervening commands. If the commander is a general officer, endorsements may be signed by the deputy commander or chief of staff. Requests which are not supported by intervening commands will be returned by the intervening command.

G-8. Compensatory measures are procedures or measures initiated in lieu of full compliance with regulatory or prescribed standards of security. Measures which are regulatory or prescribed are not compensatory. Compensatory measures must be initiated immediately upon determination that a deficient security condition exists for which a waiver or exception is required. Implementation of such measures will not be held in abeyance pending submission or approval of a request for waiver or exception. Compensatory measures are essential to ensure that standards of protection equivalent to the regulatory requirements are maintained. Failure to accomplish mandated compensatory measures will result in revocation of the applicable waiver or exception. All requests for waivers or exceptions based upon compensatory measures must specify the estimated annual cost of such measures.

G-9. Paragraph 1f of the request will include explicit information as to the status of planned corrective action to include action to be taken, estimated cost, status of the action, and anticipated completion date. If action to correct the deficiency cannot be taken, the reasons must be stated. Waiver requests that do not indicate positive steps are being taken to correct deficient conditions may be denied.

G-10. Pertinent data concerning the upgrade project designed to correct deficiencies for which relief is sought will be enclosed with all requests for waivers or requests for extension of waivers.

G-11. Deficiencies which will be corrected within 60 days for chemical sites or within 90 days for conventional sites will not require a waiver; however, commander-approved compensatory measures must be initiated immediately. This provision does not apply to security requirements mandated by ARs 190-54, and 190-59. For these regulations, deficiencies not corrected immediately, commander-approved compensatory measures will be implemented, and a request for waiver or exception will be submitted without delay.

G-12. Waivers and exceptions are not valid until approved by HQDA (DAMO-ODL). Waivers and exceptions will not be requested solely to eliminate an inconvenience or minimize expense. Waivers and exceptions will be considered individually. Blanket waivers and exceptions, i.e., covering all members or aspects of a large group or class of things, conditions, situations, etc., will not be processed. It is essential that deviations from established minimum-security requirements be subjected to intense management until full correction and compliance are achieved.

G-13. The Physical Security Waiver and Exceptions Report is automated. Waivers and exceptions are purged from the database on established expiration or revalidation dates. Therefore, it is of paramount importance that SSD is made aware of all waivers and exceptions during the course of a PSS. Waivers and exceptions must be reported through command channels for cancellation.

HEADING

OFFICE SYMBOL (MARKS NUMBER) DATE:

MEMORANDUM THRU Commander U.S. Army Materiel Command, ATTN: AMCPE-S, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001

FOR Headquarters, Department of the Army, ATTN: DAMO-ODL, 400 Army Pentagon, Washington, DC 20310-0400

SUBJECT: Request for Physical Security Waiver (or Exception)

1. Request the following physical security waiver (or exception) be granted:

a. Regulation. (Cite appropriate directive, regulation, or supplement, to include paragraph for which waiver or exception is requested.)

b. Standard. (Paraphrase the specific regulatory standard for which waiver or exception is requested.)

c. Reason standard cannot be met. (Provide specific details; include any material such as maps, photos, drawings, etc. that clearly illustrate the regulatory shortfall and why the required standard cannot or should not be implemented.)

d. Compensatory measures in effect and all costs related to those measures. (List actual measures; illustrate as required, which have been implemented.)

e. Other factors bearing on the request. (Impact on other approved waivers or exceptions, impact on resources, impact of other security shortfalls such as fencing, lighting, clear zones, and intrusion detection systems, etc.)

f. Corrective actions. (Include explicit information as to actions being taken or planned to meet regulatory standards to include estimated costs and date of completion. Include reference to POM or other resource management action to fund remedy of this shortfall.)

2. The following waivers and exceptions are currently assigned: (List by identification number and assignment date. Do not list waivers or exceptions applicable to installation or MSC directives.)

SIGNATURE (Commander)

APPENDIX H

RESPONSE TO PHYSICAL SECURITY SURVEY (PSS)/ INFORMATION SECURITY PROGRAM INSPECTION (ISPI) REPORTS

H-1. Purpose. To establish procedures for reporting corrective action to survey reports.

H-2. Definitions.

a. Deficiency -- A condition which is not accordance or in compliance with written policy.

b. Comment. Comments are used to describe conditions or actions that impact upon the overall security of the surveyed command or activity. Descriptions of waivers, exceptions, and compensatory measures may be addressed as comments.

NOTE: All findings requiring a response will be so annotated in the survey/report.

H-3. Physical Security Survey Ratings. The following physical security survey ratings are used to describe the evaluation of the inspected command/activity's overall security posture.

a. Excellent. The inspected command/activity is in near total compliance with required security standards and no major deficiencies or vulnerabilities were observed during the inspection.

b. Good. The inspected command/activity is in general compliance with required security standards. Although deficiencies (to include a limited number of major deficiencies) and vulnerabilities exist, they can be corrected in a limited period of time.

c. Marginal. The inspected command/activity's level of compliance with required security standards is at the lowest limits of acceptability. Major deficiencies/vulnerabilities exists or the total number of deficiencies is so large that the activity's overall security posture is threatened. Very positive and timely corrective actions are required to ensure the protection of AA&E, persons, property and/or facilities.

d. Poor. The inspected command/activity is in general noncompliance with required security standards. Major deficiencies/vulnerabilities exists and immediate command attention is required to ensure adequate security.

H-4. Inspected Command/Activity Responses to Inspection Surveys. The requirement for inspected commands and activities to respond to physical security surveys (PSS) will be determined by the overall rating and severity of deficiencies identified. The seriousness of deficiencies or vulnerabilities will be determined by Security Support Division (SSD) personnel while on site and reviewed by the Chief, SSD who will identify PSS response requirements. The following rules will apply:

a. Survey reports rated excellent or good (with no major deficiencies/ vulnerabilities) will require no response.

b. Good ratings with major deficiencies or vulnerabilities require response only to those deficiencies/vulnerabilities.

c. Marginal or poor ratings will require response to all deficiencies and vulnerabilities.

H-5 Responses. The inspected activity's initial response to the report will, as a minimum, contain a full and complete statement of actions taken, to date, to correct the cited conditions. For those actions considered complete, a description of the action taken will be followed by the statement, "action completed." For those which have not been completed, a target date will be provided. For actions which are expected to take 6 months or more to complete (such as work orders or construction projects), milestones will be established. Subsequent endorsements must provide the status of milestone actions. Target dates considered to be unreasonable or unrealistic will be challenged.

a. A nonconcurrence with any finding will be stated in the initial response and will be supported by a full and complete justification for the nonconcurrence. When appropriate, correspondence or messages will be attached as enclosures to the response.

b. If the surveyed command does not understand a finding, clarification should be requested. Similarly, if there are questions concerning the appropriate corrective action, these questions should be identified in the initial response.

c. SSD will, by return endorsement, indicate concurrence or nonconcurrence with the actions taken or planned, and will provide clarification or answer any questions raised in the response.

H-6. Response Procedures. The following guidelines concerning statements of corrective actin are provided.

a. Response must indicate specific action taken to correct each deficiency. Each response must provide a complete statement of corrective action(s), e.g., where a deficiency for failure to conduct an inventory of keys and locks on a quarterly basis has been cited, response must indicate that an inventory has been conducted; statements such as "procedures have been established to conduct quarterly inventories," or "personnel have been briefed on their responsibilities to conduct quarterly inventories" are not acceptable in that all actions needed to correct the condition have not been completed. In all situations, actions must be taken to correct the condition (if possible), rather than project future dates for correction; however, when immediate corrective action is not possible (requires completion of a work order request or Major Construction, Army (MCA) project), has been submitted and that a request for waiver or exception has been submitted. In this regard, the deficiency will not be considered closed until the work order request or MCA project is complete, or an approved waiver or exception is issued.

b. A response which merely states "corrected" without explaining how a deficient condition was corrected is unacceptable.

c. Vague or incomplete responses will be returned for clarification or additional information.

d. Changes to physical security plans/plant protection plans (PSP/PPP) and new or revised supplements and SOPs generated as a part of corrective action must be enclosed with the response for review and inclusion with SSD installation files.

e. All responses to survey reports must be signed by the installation commander or activity chief.

H-7. MSC Review. Security personnel at MSC headquarters will review the installations or activity's first response to the PSS for adequacy. In the event the response is determined to be inadequate or not in conformance with the above guidelines, it will be returned to the installation or activity for necessary correction or additional information. An information copy of the installation response and the MSC endorsement will be provided to SSD. The MSC will establish a new suspense (within 60 days) and SSD will adjust their suspense accordingly. All subsequent endorsements by the installation or activity will be reviewed by the MSC and will be forwarded to SSD for evaluation. All endorsements to the basic report forwarded to SSD for their evaluation will be signed by the commander, chief, or director at installation or activity level and by the commander, deputy commander, or chief of staff at MSC level. In the absence of the commander, the acting commander may sign when the signature block clearly reflects that status. However, signatures "for the commander" are not acceptable at the installation level. They are acceptable at MSC level when signed by the deputy commander or chief of staff. Responsibility to close survey/ inspection reports remains with SSD. Deficiencies that require response from the MSC will be preceded by an asterisk (*) in the PSS report. The MSC will provide a response along with the installation/activity response. If no response is required from the installation/activity, the MSC will provide only their response to SSD.

H-8. Report Closure. Compliance with the above procedures will reduce the volume of correspondence generated by elements involved in the survey closure process. Survey reports, that require a response, will not be closed with outstanding deficiencies, unless they are covered by an approved waiver or exception. Reports may be closed if next scheduled survey is within 30 days and there are outstanding deficiencies. In this situation, closing elements will state that outstanding deficiencies will be items of special interest during the next survey.